Self Attested Images for Secured Transactions using Superior SOM

Asst. Prof. N. Chenthalir Indra[1], Prof. Dr. E. Ramaraj[2],
[1] S.T. Hindu College/Computer Science Department, Nagercoil, India
[2] Alagappa University/Department of computer Science and Engineering, Karaikudi, India
Email:[1] ncigk@rediffmail.com,[2] eramaraj@rediffmail.com

***Abstract*—Separate digital signals are usually used as the digital watermarks. But this paper proposes rebuffed untrained minute values of vital image as a digital watermark, since no host image is needed to hide the vital image for its safety. The vital images can be transformed with the self attestation. Superior Self Organized Maps is used to derive self signature from the vital image. This analysis work constructs framework with Superior Self Organizing Maps (SSOM) against Counter Propagation Network for watermark generation and detection. The required features like robustness, imperceptibility and security was analyzed to prove that which neural network is appropriate for mining watermark from the host image. SSOM network is proved as an efficient neural trainer for the proposed watermarking technique. The paper presents one more contribution to the watermarking area.**

***Index Terms*— Superior Self Organizing Maps, Counter Propagation Network, mining, watermarking, embedding, host image, vital image.**

I. Introduction

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The information to be embedded is called a digital watermark. The signal where the watermark is to be embedded is called the host signal. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. A watermarking system is usually divided into three distinct steps, embedding, attack and detection. Embedding signal produces watermarked signal, modifications on these signal by any intruders are called attacks.

Neural algorithm in watermarking research is common today. But the early methods used Neural Network logics for finding and maximizing the strength of watermark, embedding and detecting processes. The following section II states the references for the existing contribution of neural networks in watermarking. Common algorithms used for watermarking are Counter Propagation Network (CPN), Back Propagation Network (BPN), Hopfield Neural Network and Radial Base Function network (RBF). The major role was done by Full Counter Propagation Network (FCPN) and Back Propagation Network.The proposed system gives new dimension to the watermarking field. Existing techniques use host image (cover image) to hide the authorized image for further secured transformation. Here maintaining the robustness of the embedded image is more important. In this analysis the watermarked image is an essential part of communication. In this system the vital image is transferred in open with its self signature. The actual image, which is to be transferred from one end to other end, is known as vital image. At the other end this signature value is tested for the authorization. Hence the vital image referred to in this scheme is host image. The self signature value, which is generated from the same image by using the Superior Self Organizing Maps (SSOM), is called as digital watermark value. For embedding, the Discrete Wavelet Transform (DWT) is used. For this process SSOM is the significant algorithm. This is proved by comparing the system with CPN based similar framework.

This paper proposes SSOM Neural Network for watermarking. Section III describes the SSOM. Watermark value generation from host color image and the watermark extraction from watermarked image are done here by SSOM. Generation and detection processes are presented in section IV. The same framework of watermark generation and detection are done with both CPN and SSOM and the robustness, imperceptibility and security of watermark is analyzed in section V.

II. Review on Existing Neural Network Based Watermarking

In the paper [11], neural network was used to learn the relationship between the embedded watermark and the watermarked image. The relationship learnt by the neural network is then used as a digital signature in the extraction process. In [9], a technique presents the method of deciding watermarking strength in DCT domain using artificial neural network.

A BPN model is used to learn the relationship between the watermark and the watermarked image [7]. Zhang [6] proposed a blind watermarking algorithm using Hopfield neural network and then analyzed the watermarking capacity based on the neural network. Chang [4] presented a specific designed FCPN for digital image watermarking. Different from the traditional methods, the watermark was embedded in the synapses of the FCNN instead of the cover image. [1] Proposed a new blind watermarking scheme in which a watermark was embedded into the DWT domain. It also utilized RBF Neural network to learn the characteristic of the image, using which, the watermark would be embedded and extracted. The embedding scheme resulted in a good quality watermarked image.Yi [10] proposed a novel digital watermarking scheme basedon improved BPN for color images

DOI: 01.IJIT.3.1.1023

The watermark was embedded into the discrete wavelet domain of the original image and extracted by training the BPN which learnt the characteristics of the image. Huang [12] proposed a novel watermarking technique based on image features and neural networks. Here, the Arnold transform is used to increase the security of watermark. The BPN is applied to improve its imperceptibility and robustness. C.-Y. Chang et al. [5] used a FCNN for copyright protection where the ownership information was embedded and detected by a specific FCNN.

The above mentioned papers exhibit the neural networks contribution in the field of watermarking. Most of the systems used CPN, BPN and RBF algorithms. However this paper makes an attempt with SSOM, not for embedding and detention of watermark as in the early techniques, but for watermark value generation and detection.

III. Required Techniques

The scheme proposed in this extension research process uses SSOM as its main algorithm. SSOM is an unsupervised competitive learner, which is used for mining process. Mining means extracting useful information from the existing data. SSOM's learning capacity is very high than the traditional Kohonen Self Organizing Maps (KSOM), which uses the Euclidean distance as its winner selector. More over the FCPN in the early papers which has proved its efficiency is used KSOM training in its first phase and second phase uses Gross berg's logic. The first phase plays an important role in FCPN procedure.SSOM proved its efficiency against traditional KSOM in the early papers [2] [3]. Hence the improvised Superior SOM is the best choice for this process. No neural process was used for digital watermark making. Early methods used neural networks for finding and maximizing strength of watermark, watermark embedding and detection processes. Where as this paper applies SSOM for watermark signal making from host image and watermark detection from transformed watermarked image.

A. Superior SOM

Step0: Weights are initialized with random method or by having previous knowledge of pattern distribution. Topological neighborhood parameters are set. Learning rate (0.6 to 1) parameter is set.

Step1: The steps 2 – 8 are repeated by testing the condition.

Step2: For each input vector x, do steps 3– 5

Step3: For each j , compute $d(j)$ by using any one of the following distance measures Eqns.(1) or (2).

a) Manhattan Distance:

$$d\left(x\,,\,y\right) = \sum_{i=1}^{M} \left| x_i - y_i \right| \qquad (1)$$

b) Lee distance:

$$d_m(x, y) = \sum_{i=1}^{M} \left\{ \left| x_i - y_i \right|, q - \left| x_i - y_i \right| \right\} \qquad (2)$$

Step4: Index J is found such that d (j) is a minimum.

Step5: For units j within a specified neighborhood of J and for all i, $W_{ij(new)} = W_{ij(old)} + \alpha \left\lfloor X_i - W_{ij(old)} \right\rfloor$

Step6: The learning rate is updated.

Step7: The Radius of topological is reduced at specified times

Step8: The condition is verified. Condition is based on the size of the input.

SSOM exactly imitates human neural learning logic. Hence trivial imbalanced values can be identified through the analysis. These insignificant map elements in SSOM network is determined and used as watermark values.

B. Discrete Wavelet Transformation

For embedding process the scheme uses Discrete Wavelet Transformation (DWT). The first DWT was invented by the Hungarian mathematician Alfred Haar. For an input represented by a list of 2n numbers, the Haar wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale: finally resulting in 2n " 1 differences and one final sum. The wavelet transform decomposes input image into four components namely LL, HL, LH and HH. The lowest resolution level LL consists of the approximation part of the original image. The remaining three resolution levels consist of the detail parts and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies. For one level decomposition, the discrete two-dimensional wavelet transform of the image function f(x,y) can be written as

$$LL = \left[\left(f\left(x.y\right)*\phi(-x)\phi(-y)\right)(2n,2m)\right]_{(n,m)\in z^2}$$

$$LH = \left[\left(f\left(x.y\right)*\phi(-x)\psi(-y)\right)(2n,2m)\right]_{(n,m)\in z^2}$$

$$HL = \left[\left(f\left(x.y\right)*\psi(-x)\phi(-y)\right)(2n,2m)\right]_{(n,m)\in z^2}$$

$$HH = \left[\left(f\left(x.y\right)*\psi(-x)\psi(-y)\right)(2n,2m)\right]_{(n,m)\in z^2}$$

Where $\phi\,(t)$ is a low pass scaling function and $\psi\,(t)$ is the associated band pass wavelet function. In the proposed technique, embedding and extraction of watermark takes place in the high frequency component. For a one level decomposition, the discrete two-dimensional wavelet transform of the image function f(x, y) is found in [8] [13]. DWT transform based watermarking scheme is robust against many common image attacks. The analysis results proved robustness very well.

C. Counter Propagation Network

The Counter Propagation Network is a hybrid network. This section explains its algorithm because the same is used to compare the strength of the proposed system. CPN is a neural network model developed by Robert Hecht-Nielsen [14]. There is an input layer, a hidden layer (called the Kohonen layer) and an output layer called the Grossberg layer. The network is fully feed forward connected. Training takes place in two stages.

Stage 1:

- First, the Kohonen layer is trained in an unsupervised manner.
- This trains the processing elements in the layer to differentiate between different input vectors.

Stage 2:

- The second phase trains the Grossberg layer in a supervised manner.
- This trains the Grossberg layer to associate an output vector with each recognised input vector.
- Once trained, the network will output an appropriate output vector for any given input vector.

IV. Proposed Watermarking Scheme

The following algorithm presents overall structure of the proposed technique.

A. Preprocessing the Image:

1) The input images are collected. The host image is selected for watermarking. Read its RGB values (3-D) as $X(x, y, z)$

2) Its Red, Green and Blue color attributes are extracted in separate 2-D spaces Xr*(x,y), Xg(x,y) and Xb(x,y)* respectively.

B. Water Mark Value Mining:

1) The SSOM network is set with three layers. (Input, three hidden and output with two dimensional space matrix).

2) Its weight vectors are initialized with integer numbers by using any existing auto random number generator function. Red, green and blue related SOM weight vectors are *Wr(x,y), Wg(x,y) and Wb(x,y)* respectively (random numbers between 0 and 255 integer values).

3) Learning rate a is initialized as 0.8 (this threshold value may vary between 0.5 and 1.0).

4) Red, Green and Blue feature 2-D matrix values are supplied to the input layer of SOM network. The network is trained by using the feasible measures given in the SSOM. SSOM uses *Manhattan measure* in the Eqn. (1) or *Lee distance* Eqn. (2) instead of Euclidian distance

5) Trained RGB attributes are obtained in the output layer.

6) The difference between input values and trained values of each color are found. The resultant values are accepted as digital watermark values. Thus this process brings out three sets of digital watermarks.

C. Embedding Watermark:

1) 1-level DWT is activated to original image's red vectors.

2) The red attribute watermark is embedded in the high frequency component HH of DWT.

3) Inverse wavelet transform is executed to obtain the watermarked red features.

4) The above three steps are repeated for other two green and blue colors too.

D. Watermarked Image Accumulation:

1) The watermarked 2-D space values of each color are collected.

2) They are combined together into 3-D space data type.

3) The resultant 3-D image values are stored using .jpg format. (compressed watermarked host image is ready for transmission).

E. Watermark Detection and Separation:

Projected watermarking proposal is capable of mine watermark information in the absence of the original image or secret key. Hence it is unsighted watermarking.

1) One level DWT is triggered to the destination image and the embedded watermark is taken away from the HH sub band.

2) Watermark from the transferred image is regenerated by using SSOM neural logic as mentioned in the generation algorithm.

Quality of transferred watermarked image is analyzed by using PSNR measure given in Eqn. (3).

$$PSNR = 10 \log_{10}\left(\frac{255^{2}}{MSE}\right) \qquad (3)$$

Where, MSE is Mean Squared Error between original image and watermarked image. Similarity ratio between the host image and watermarked image is calculated by using *Jaccard similarity* measure given in the Eqn. (4). The similarity ratio (SR) is 1 for the exactly same images and 0 for the entirely different images. This paper accepts the range from 0.8 to 1 as the best validity of similarity ratio.

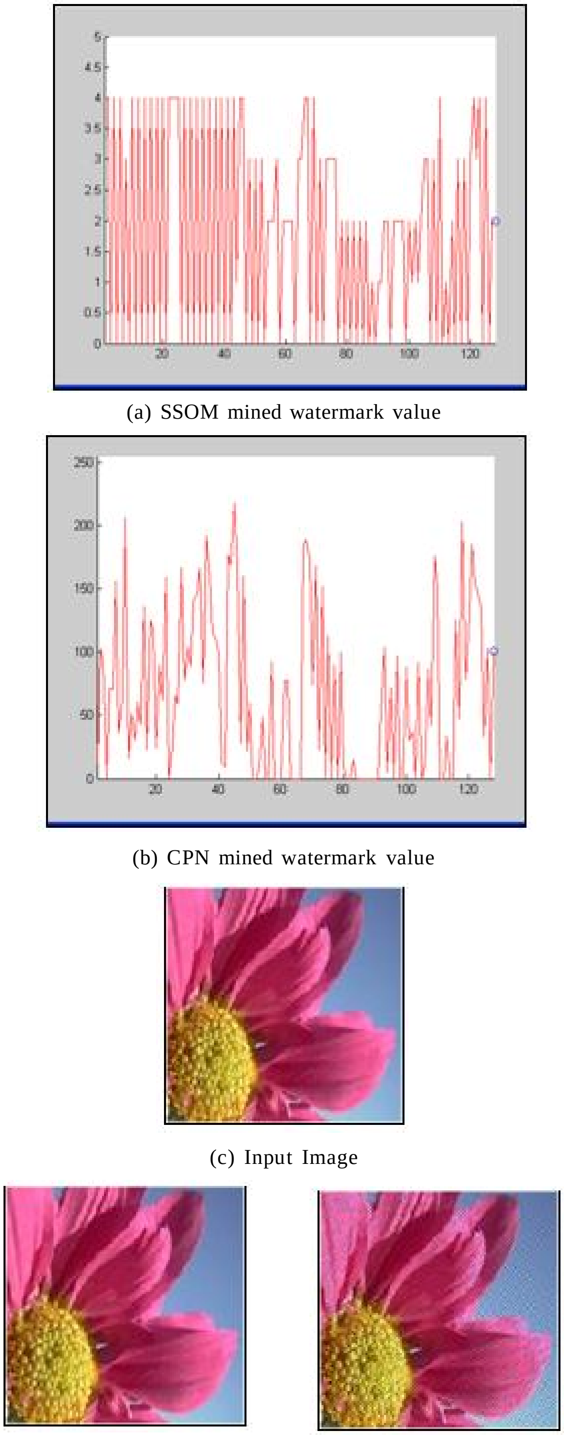
$$sim(x_i, w_j) = \frac{\sum_{h=1}^{k} x_{ih} w_{jh}}{\sum_{h=1}^{k} x_{ih}^{2} + \sum_{h=1}^{k} w_{jh}^{2} - \sum_{h=1}^{k} x_{ih} w_{jh}} \qquad (4)$$

V. Analysis on SSOM Watermarking

The framework was constructed to conduct analysis on proposed watermarking scheme with both the networks, Superior Self Organizing Maps (SSOM) and Counter propagation Network (CPN). The results of watermarking using SSOM were compared with the same results with CPN. Every aspect of watermarking features such as robustness, imperceptibility and security was analyzed. The host image was selected and given as input to the watermark value mining process. The RGB feature values are extracted and three sets of 2-D matrix values are constructed according to the image pattern. These RGB 2-D plane are trained by SSOM algorithm with its authenticated initial settings. The trained network weight vectors are compared with host image color pixel values Minute significant values are identified as digital watermark. The digital watermark is embedded by using single level DWT.

The Table I shows the quality of watermarked image. Superior SOM based watermark embedding yields reasonable PSNR value and high-quality SR value. Whereas CPN based watermark embedding gives away lower PSNR & SR values than the SSOM. No techniques can guess these water mark values because the SOM is unsupervised learner and moreover the experiment uses random numbers to initialize the weight vector of hidden layer. Results were analyzed with two modes one by Counter Propagation Network (CPN) and

DOI: 01.IJIT.3.1.1023



(a) SSOM mined watermark value

(b) CPN mined watermark value

(c) Input Image

(d) SSOM-Watermarked

(e) CPN– Watermarked

Fig. 1. (a)&(b)Digital Watermark Values (c) Host Image (d) & (e) Watermark embedded image

other with proposed Superior SOM.Fig. 1(e) is the evidence for the watermark embedded image which is visually degraded with CPN. But with Superior SOM the watermarked image is impeccable, which is given in the Fig. 1 (d). The watermark values mined from host image is given in the Fig. 1 (a) & (b). The CPN based watermark value is of its high RGB range (1 to 255). While the SSOM generated digital watermark range is very small (0 to 4.5). Embedding lower values produces imperceptible watermarking. If the digital value is high the visual degradation is unavoidable. Fig. 1 (a) & (b) x-axis denotes image size (128 x 128). Y-axis gives RGB value range from 1 to 255.The robustness of the watermark is verified through the watermark detection process. At the destination side transferred watermarked image was collected and detection technique was applied to separate the watermark value from the image. No supporting keys are needed to regenerate watermark because the SSOM is a self organizing network. It regenerates the watermark value with its own training process.

Table I. Type Sizes For Camera-Ready Papers

Image	CPN Quality Ratio		Superior SOM Quality Ratio	
	PSNR	SR	PSNR	SR
Watermarked	38	0.89	53.7	0.99
Compressed (WM)	37	0.9	54	0.99

Table II. Similarity Between Digital Watermark And Detected Watermark

Types of attacks	Detected watermark robustness (CPN)		Detected watermark robustness (Superior SOM)	
	PSNR	SR	PSNR	SR
No attacks	34.9	0.4	54.6	0.82
Compressed(WM)	34.8	0.41	53.3	0.7
Gaussian	34.7	0.38	51.2	0.5
Poisson	34.8	0.39	53.1	0.68
Salt & Pepper	34.7	0.39	52	0.63
Speckle	34.6	0.37	51	0.52
Damaged	35.6	0.34	52.2	0.52

The detected watermark value is compared with the original watermark value by PSNR and SR calculations and the results are tabulated in the Table II. SSOM based watermark is robust. Even after the noise attack SSOM can detect the watermark values with acceptable PSNR & SR values. The CPN based watermark detector fails to find the good quality watermark even with image, which is not attacked by any sources. Its SR is very low. SSOM based watermark detector produces first-rate PSNR and SR values. The Fig. 2 clearly displays that the SSOM robustness is higher than the CPN based watermarking. If the CPN is used the watermark detection process fails to retrieve good quality watermark signal. On the other hand SSOM retrieves the watermark after the malicious attacks. But the strength of attack degrades the watermark's similarity ratio to optimum level.Security based analysis results are put on show in the Table III. Watermark was detected and removed from the transferred image. Then the watermark removed image was compared with the authorized image at the destination node by calculating PSNR and SR. The watermarked transferred image with no attack produces real quality image with high level PSNR and SR values. Specifically its similarity ratio is very accurate (SR=1). If the mistreat of the watermarked image was handled while transferring the image, the real image with '**1**' as its SR value can not be produced. Thus the proposed system promises the authorization confirmation.

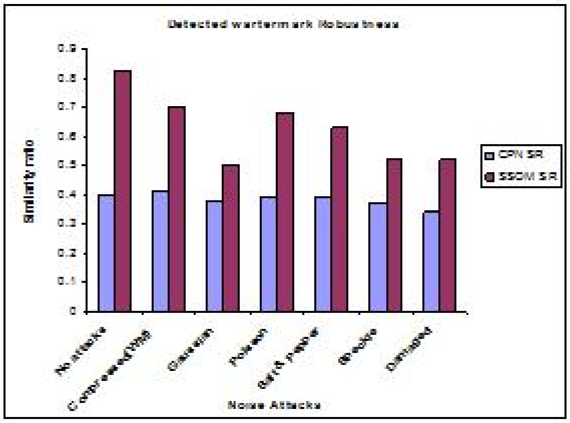
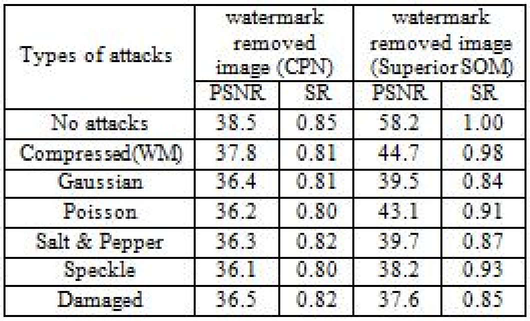


Fig. 2. Robustness Comparison between CPN and SSOM watermark with various attacks

TABLE III. RECEIVED IMAGE QUALITY AFTER THE REMOVAL OF WATERMARK



Types of attacks	watermark removed image (CPN)		watermark removed image (Superior SOM)	
	PSNR	SR	PSNR	SR
No attacks	38.5	0.85	58.2	1.00
Compressed(WM)	37.8	0.81	44.7	0.98
Gaussian	36.4	0.81	39.5	0.84
Poisson	36.2	0.80	43.1	0.91
Salt & Pepper	36.3	0.82	39.7	0.87
Speckle	36.1	0.80	38.2	0.93
Damaged	36.5	0.82	37.6	0.85

CONCLUSIONS

In the existing watermarking techniques neural algorithms are used to embed watermark image in the host image. In this proposed system no separate host image is used. The vital image which is to be transferred is used as host image too. Since the self signature is unique for each image, watermark value regeneration is only possible from the original image. So the proposed image transformation endorses that no one can claim otherwise for the image. If the malicious attack is happened during the transformation, the attacked image can be identified with confirmation test at the destination side. The image with similarity ratio '1' can not be got back from the watermarked image if it is attacked.

REFERENCES

[1] Cheng-Ri Piao, Suenghwa Beack, Dong-Min Woo and Seung-Soo Han, "A Blind Watermarking Algorithm based on HVS and RBF Neural Network for Digital Image", ICNC 2006,Part 1, LNCS 4221, pp. 493-496, 2006.

[2] Chenthalir Indra N, Dr. E. Ramaraj: "Magnitude of Self Systematizing Resemblance Measures in Knowledge Mining": In Software Technology and Engineering Proceedings of the International Conference on ICSTE 2009,pp.239-43,DOINo:10.1142/97889814289986_0044, World Scientific Publications.

[3] Chenthalir Indra N and Dr. E. Ramaraj, "Similar - Dissimilar Victor Measure Analysis to Improve Image Knowledge Discovery Capacity of SOM ".: In International Conference on Information and Communication Technologies, ICT 2010 Proceedings. Volume 101, Part 2, pp.389-393, DOI: 10.1007/978-3-642-15766-0_61. published by Springer-Verlag.

[4] Chuan-Yu Chang and Sheng-Jyun Su, "The Application of a Full Counterpropagation Neural Network to Image Watermarking", 2005.

[5] Chuan-Yu Cahng, Hung-Jen Wang, Sheng-Jyun Su, "Copyright authentication for images with a full ounterpropagation neural network", Expert Systems with Applications 37, 2010.

[6] Fan Zhang, Hongbin Zhang, "Applications of Neural Network to Watermarking Capacity", International Symposium on Communications and Information Technologies, October 26-29, 2004.

[7] Jun Zhang, Nenchao Wang, Feng Xiong, "Hiding a Logo Watermark into the Multiwavelet Domain using Neural Networks", In the Proceedings of the 14th IEEE International Conference on Tools with Artificial Intelligence, 2002.

[8] Kumar, S., Raman, B., Thakur, M.: "Real Coded Genetic Algorithm based Stereo image Watermarking". In: IJSDIA 1(1),pp.23–33 (2009).

[9] Mei Shi-chun, Li Ren-hou, Dang Hong-mei, Wang Yunkuan, "Decision of Image Watermarking strength based on Artificial Neural Networks", In the Proceedings of the 9th International Conference on Neural Information Processing, Vol. 5, 2002.

[10] Qianhui Yi and Ke Wang, "An Improved Watermarking method based on Neural Network for Color Image", In the Proceedings of the 2009 IEEE International Conference on Mechatronics and Automation, August 9-12, 2009.

[11] Pao-Ta Yu, Hung-Hsu Tsai, Jyh-Shyan Lin, " Digital watermarking based on neural networks for color images", Signal Processing, pp 663-671, 2001.

[12] Song Huang, Wei Zhang, "Digital Watermarking based on Neural Network and Image Features", 2nd International Conference on Information and Computing Science, 2009.

[13] S.S. Sujatha and M. Mohamed Sathik "Feature Based Watermarking Algorithm by Adopting Arnold Transform" ICT 2010, CCIS 101, pp. 78–82, 2010. © Springer-Verlag Berlin Heidelberg 2010.

[14] Valluru B. Rao and Hayagriva V.Rao "Neural Networks & FuzzyLogic", ISBN 81-7029-694-3. BPB Publications. Second edition.